CLAIMS

1. A method for establishing an encrypted communication channel between a first apparatus and a second apparatus by using a session management apparatus, comprising the steps of:

establishing a first encrypted communication channel between the session management apparatus and the first apparatus by performing mutual authentication between the session management apparatus and the first apparatus;

establishing a second encrypted communication channel between the session management apparatus and the second apparatus by performing mutual authentication between the session management apparatus and the second apparatus; and

exchanging key information between the first apparatus and the second apparatus via the first encrypted communication channel and the second encrypted communication channel so as to establish an encrypted communication channel between the first apparatus and the second apparatus.

2. A method for establishing an encrypted communication channel between a first apparatus and a second apparatus by using a session management apparatus, wherein:

the session management apparatus and the first apparatus exchange key information for encrypted communication, and performs mutual authentication so as to establish a first encrypted communication channel between the session management apparatus and the first apparatus;

the session management apparatus and the second apparatus exchange key information for encrypted communication, and performs mutual authentication so as to establish a second encrypted

communication channel between the session management apparatus and the second apparatus;

the first apparatus sends, to the session management apparatus via the first encrypted communication channel, a connection request message destined for the second apparatus including key information used for encrypted communication between the first apparatus and the second apparatus, and the session management apparatus sends the connection request message to the second apparatus via the second encrypted communication channel; and

the second apparatus sends, to the session management apparatus via the second encrypted communication channel, a response message including key information used for encrypted communication between the first apparatus and the second apparatus in response to receiving the connection request message, and the session management apparatus sends the response message to the first apparatus via the first encrypted communication channel.

3. A session management apparatus for establishing an encrypted communication channel between a first apparatus and a second apparatus, the session management apparatus comprising:

a part for exchanging key information for encrypted communication with the first apparatus, and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel between the session management apparatus and the first apparatus;

a part for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second apparatus so as to establish a second encrypted communication channel between the session management apparatus and the second apparatus;

a part for receiving, from the first apparatus via the first encrypted communication channel, a connection request message to the second apparatus that includes key information for encrypted communication between the first apparatus and the second apparatus, and transferring the connection request message to the second apparatus via the second encrypted communication channel; and

a part for receiving, from the second apparatus via the second encrypted communication channel, a response message that includes key information for encrypted communication between the first apparatus and the second apparatus, and transferring the response message to the first apparatus via the first encrypted communication channel.

4. The session management apparatus as claimed in claim 3, the session management apparatus further comprising:

a part for performing message communications between the first apparatus and the session management apparatus and between the second apparatus and the session management apparatus by using Session Initiation Protocol.

5. The session management apparatus as claimed in claim 3, the session management apparatus further comprising:

a part for receiving a name and an address of the first apparatus via the first encrypted communication channel, and registering the name and the address of the first apparatus in a storage device of the session management apparatus;

a part for receiving a name and an address of the second apparatus via the second encrypted communication channel, and registering the name and

the address of the second apparatus in the storage device; and

a name resolution part for obtaining the address of the second apparatus from the name of the second apparatus included in the connection request message sent from the first apparatus.

6. The session management apparatus as claimed in claim 3, the session management apparatus further comprising:

a part for determining whether the first apparatus is permitted to access the second apparatus by referring to access permission information stored in the session management apparatus when the session management apparatus receives the connection request message from the first apparatus, and rejecting access to the second apparatus by the first apparatus if the first apparatus is not permitted to access the second apparatus.

7. The session management apparatus as claimed in claim 3, the session management apparatus further comprising:

a part for receiving a public-key from the first apparatus via the first encrypted communication channel; and

a part for generating a public-key certificate for the received public-key, and sending the public-key certificate to the first apparatus via the first encrypted communication channel.

8. The session management apparatus as claimed in claim 7, wherein the session management apparatus includes a server for establishing the first encrypted communication channel to the first apparatus, and an apparatus that is connected to the

server and that generates and manages public-key certificates.

9. The session management apparatus as claimed in claim 3, the session management apparatus further comprising:

a part for receiving a public-key of the first apparatus via the first encrypted communication channel;

a part for storing the received public-key in its storage device; and

a part for sending the public-key of the first apparatus via the second encrypted communication channel to the second apparatus.

10. The session management apparatus as claimed in claim 9, wherein the session management apparatus includes a first apparatus for establishing the first encrypted communication channel and the second encrypted communication channel, and a second apparatus that is connected to the first apparatus and that manages public-keys.

11. The session management apparatus as claimed in claim 3, the session management apparatus further comprising:

a storage device for storing a name of the first apparatus and identification information of the first encrypted communication channel wherein the name of the first apparatus and the identification information are associated with each other; and

a part for determining whether a name included in the connection request message received from the first apparatus is correct by comparing the name included in the connection request message with the name that is stored in the storage device and

that is associated with the identification information of the first encrypted communication channel.

12. The session management apparatus as claimed in claim 11, wherein, if the session management apparatus determines that the name of the first apparatus included in the connection request message is not correct, the session management apparatus sends an error message to the first apparatus.

13. The session management apparatus as claimed in claim 3, wherein the connection request message received from the first apparatus includes a first header indicating reliability of a route between the first apparatus and the session management apparatus, the session management apparatus further comprising:

a part for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the connection request message, and sending the connection request message to the second apparatus via the second encrypted communication channel.

14. The session management apparatus as claimed in claim 13, wherein the first header includes an address of the first apparatus, and in response to receiving the first header, the session management apparatus determines validity of the first header by comparing the address included in the first header and an address of the first apparatus.

15. An apparatus that establishes an

encrypted communication channel to a second apparatus by using a session management apparatus, the apparatus comprising:

a part for exchanging key information for encrypted communication with the session management apparatus, performing mutual authentication with the session management apparatus so as to establish a first encrypted communication channel between the apparatus and the session management apparatus; and

a part for sending, to the session management apparatus via the first encrypted communication channel, a connection request message including key information for encrypted communication between the apparatus and the second apparatus, and receiving, from the second apparatus via the session management apparatus, a response message including key information for encrypted communication between the apparatus and the second apparatus so as to establish a second encrypted communication channel between the apparatus and the second apparatus.

16. The apparatus as claimed in claim 15, wherein: when the apparatus is accessed by a third apparatus, the apparatus establishes the first encrypted communication channel and establishes the second encrypted communication channel by using the first encrypted communication channel; and

the apparatus receives data from the second apparatus via the second encrypted communication channel between the apparatus and the second apparatus, and sends the data to the third apparatus.

17. The apparatus as claimed in claim 15, wherein: when the apparatus is accessed by a third apparatus, the apparatus establishes the second

encrypted communication channel by using the first encrypted communication channel; and

the apparatus receives data from the second apparatus via the second encrypted communication channel between the apparatus and the second apparatus, and sends the data to the third apparatus.

18. The apparatus as claimed in claim 16 or 17, wherein the apparatus has a table including at least one connection destination to which the third apparatus is permitted to connect, and the apparatus sends the at least one connection destination to the third apparatus when the third apparatus accesses the apparatus, and receives a selected connection destination from the third apparatus.

19. A computer program for causing a computer to function as a session management apparatus that is used for establishing an encrypted communication channel between a first apparatus and a second apparatus that are connected to a communication network, the computer program comprising:

program code means for exchanging key information for encrypted communication with the first apparatus, and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel between the computer and the first apparatus;

program code means for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second apparatus so as to establish a second encrypted communication channel between the computer and the second apparatus;

program code means for receiving, from the first apparatus via the first encrypted communication channel, a connection request message to the second apparatus that includes key information for encrypted communication between the first apparatus and the second apparatus, and transferring the connection request message to the second apparatus via the second encrypted communication channel; and

program code means for receiving, from the second apparatus via the second encrypted communication channel, a response message that includes key information for encrypted communication between the first apparatus and the second apparatus, and transferring the response message to the first apparatus via the first encrypted communication channel.

20. The computer program as claimed in claim 19, the computer program further comprising:

program code means for receiving a public-key from the first apparatus via the first encrypted communication channel; and

program code means for generating a public-key certificate for the received public-key, and sending the public-key certificate to the first apparatus via the first encrypted communication channel.

21. The computer program as claimed in claim 19, the computer program further comprising:

program code means for receiving a public-key of the first apparatus via the first encrypted communication channel;

program code means for storing the received public-key in a storage device; and

program code means for sending the public-

key of the first apparatus via the second encrypted communication channel to the second apparatus.

22. A computer program for causing a computer to function as an apparatus that establishes an encrypted communication channel to a second apparatus by using a session management apparatus, the computer program comprising:

program code means for exchanging key information for encrypted communication with the session management apparatus, performing mutual authentication with the session management apparatus so as to establish a first encrypted communication channel between the computer and the session management apparatus; and

program code means for sending, to the session management apparatus via the first encrypted communication channel, a connection request message including key information for encrypted communication between the apparatus and the second apparatus, and receiving, from the second apparatus via the session management apparatus, a response message including key information for encrypted communication between the apparatus and the second apparatus so as to establish a second encrypted communication channel between the apparatus and the second apparatus.

23. The computer program as claimed in claim 19, the computer program further comprising:

program code means for storing a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other; and

program code means for determining whether

a name included in the connection request message received from the first apparatus is correct by comparing the name included in the connection request message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel.

24. The computer program as claimed in claim 19, wherein the connection request message received from the first apparatus includes a first header indicating reliability of a route between the first apparatus and the session management apparatus, the computer program further comprising:

program code means for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the connection request message, and sending the connection request message to the second apparatus via the second encrypted communication channel.

25. A method for establishing an encrypted communication channel between a first apparatus and a second apparatus, wherein:

a public-key management apparatus and the first apparatus exchange key information used for encrypted communication, and the public-key management apparatus and the first apparatus perform mutual authentication so that a first encrypted communication channel is established;

the first apparatus generates a secret key and a public-key, and sends the public-key to the public-key management apparatus via the first encrypted communication channel;

the public-key management apparatus generates a public-key certificate for the received

public-key, and sends the public-key certificate to the first apparatus via the first encrypted communication channel; and

the first apparatus sends the public-key certificate to the second apparatus so that a second encrypted communication channel using the public-key between the first apparatus and the second apparatus is established.

26. A method for establishing an encrypted communication channel between a first apparatus and a second apparatus, wherein:

a public-key management apparatus and the first apparatus exchange key information used for performing encrypted communication, and the public-key management apparatus and the first apparatus perform mutual authentication so that a first encrypted communication channel is established;

the public-key management apparatus and the second apparatus exchange key information used for encrypted communication, and the public-key management apparatus and the second apparatus perform mutual authentication so that a second encrypted communication channel is established;

the first apparatus generates a secret key and a public-key, and sends the public-key to the public-key management apparatus via the first encrypted communication channel;

the public-key management apparatus stores the received public-key in its storage device, and the second apparatus obtains the public-key from the public-key management apparatus via the second encrypted communication channel so that a third encrypted communication channel using the public-key between the first apparatus and the second apparatus is established.

27. A public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus, the public-key management apparatus comprising:

a part for exchanging key information for encrypted communication with the first apparatus, and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel;

a part for receiving a public-key from the first apparatus via the first encrypted communication channel; and

a part for generating a public-key certificate for the received public-key, and sending the public-key certificate to the first apparatus via the first encrypted communication channel.

28. The public-key management apparatus as claimed in claim 27, wherein the public-key management apparatus includes a server for establishing the first encrypted communication channel to the first apparatus, and an apparatus that is connected to the server and that generates and manages public-key certificates.

29. The public-key management apparatus as claimed in claim 27 or 28, wherein the public-key management apparatus further includes a part for performing message communications between the first apparatus and the public-key management apparatus by using Session Initiation Protocol.

30. A public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus, the public-key

management apparatus comprising:

a part for exchanging key information for encrypted communication with the first apparatus, and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel;

a part for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second apparatus so as to establish a second encrypted communication channel;

a part for receiving a public-key of the first apparatus via the first encrypted communication channel;

a part for storing the received public-key in its storage device; and

a part for sending the public-key of the first apparatus via the second encrypted communication channel to the second apparatus.

31. The public-key management apparatus as claimed in claim 30, wherein the public-key management apparatus includes a first apparatus for establishing the first encrypted communication channel and the second encrypted communication channel, and a second apparatus that is connected to the first apparatus and that manages public-keys.

32. The public-key management apparatus as claimed in claim 30 or 31, the public-key management apparatus further comprising:

a part for performing message communications between the first apparatus and the public-key management apparatus and between the second apparatus and the public-key management apparatus by using Session Initiation Protocol.

33. A computer program for causing a computer to function as a public-key management apparatus for managing public-keys, the computer program comprising:

program code means for exchanging key information for encrypted communication with a first apparatus, and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel;

program code means for receiving a public-key from the first apparatus via the first encrypted communication channel; and

program code means for generating a public-key certificate for the received public-key, and sending the public-key certificate to the first apparatus via the first encrypted communication channel.

34. A computer program for causing a computer to function as a public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus, the computer program comprising:

program code means for exchanging key information used for encrypted communication with the first apparatus, and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel;

program code means for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second apparatus so as to establish a second encrypted communication channel;

program code means for receiving a public-key of the first apparatus via the first encrypted communication channel;

program code means for storing the received public-key in a storage device; and

program code means for sending the public-key of the first apparatus via the second encrypted communication channel to the second apparatus.

35. A session management apparatus that can connect to a first apparatus and a second apparatus over a network, the session management apparatus comprising:

a part for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus, and storing a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other;

a part for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus;

a part for receiving a message including a name of the first apparatus via the first encrypted communication channel;

a part for determining whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel; and

a part for sending the message to the second apparatus via the second encrypted communication channel.

36. The session management apparatus as claimed in claim 35, wherein, if the session management apparatus determines that the name of the first apparatus included in the message is not correct, the session management apparatus sends an error message to the first apparatus.

37. A session management apparatus that can connect to a first apparatus and a second apparatus over a network, the session management apparatus comprising:

a part for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus;

a part for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus;

a part for receiving, from the first apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus; and

a part for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sending the message to the second apparatus via the second encrypted communication channel.

38. The session management apparatus as claimed in claim 37, wherein the first header includes an address of the first apparatus, and in response to receiving the first header, the session management apparatus determines validity of the

first header by comparing an address included in the first header and an address of the first apparatus.

39. The session management apparatus as claimed in claim 35, wherein the message is based on Session Initiation Protocol.

40. A method for transferring a message among a first apparatus, a session management apparatus and a second apparatus each connected to a network, wherein:

the session management apparatus and the first apparatus perform mutual authentication to establish a first encrypted communication channel between the session management apparatus and the first apparatus, and the session management apparatus stores a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other;

the session management apparatus and the second apparatus performs mutual communication to establish a second encrypted communication channel between the session management apparatus and the second apparatus;

the first apparatus sends a message including a name of the first apparatus via the first encrypted communication channel to the session management apparatus;

the session management apparatus determines whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted

communication channel; and

the session management apparatus sends the message to the second apparatus via the second encrypted communication channel.

41. A method for transferring a message among a first apparatus, a session management apparatus and a second apparatus each connected to a network, wherein:

the session management apparatus and the first apparatus perform mutual authentication to establish a first encrypted communication channel between the session management apparatus and the first apparatus;

the session management apparatus and the second apparatus perform mutual communication to establish a second encrypted communication channel between the session management apparatus and the second apparatus;

the first apparatus sends, to the session management apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus; and

the session management apparatus adds a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sends the message to the second apparatus via the second encrypted communication channel.

42. A computer program for causing a computer to function as a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the computer program comprising:

program code means for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus, and storing a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other;

program code means for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus;

program code means for receiving a message including a name of the first apparatus via the first encrypted communication channel;

program code means for determining whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel; and

program code means for sending the message to the second apparatus via the second encrypted communication channel.

43. A computer program for causing a computer to function as a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the computer program comprising:

program code means for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first

apparatus;

program code means for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus;

program code means for receiving, from the first apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus; and

program code means for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sending the message to the second apparatus via the second encrypted communication channel.